UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**No. 2:17-cr-00047-AKK-TMP**
	)	
KEVIN MITCHELL MALDONADO,	)	
Defendant.	)	

SENTENCING MEMORANDUM

COMES NOW the United States of America, by and through Acting United States Attorney Robert O. Posey and the undersigned Assistant United States Attorney, and submits this sentencing memorandum for the Court's consideration in determining an appropriate sentence for Defendant **KEVIN MITCHELL MALDONADO**. For the reasons stated below, the United States recommends a sentence of six months' incarceration, at the high-end of the advisory United States Sentencing Guidelines range, three years supervised release with certain special conditions, and appropriate restitution.

INTRODUCTION

Pursuant to an Information and Plea Agreement filed on January 26, 2017, the defendant, **KEVIN MITCHELL MALDONADO**, agreed to certain facts and pled guilty to one count of Accessing a Protected Computer without Authorization in Furtherance of a Criminal or Tortious Act, in violation of 18 U.S.C. §§ 1030(a)(2)

and (c)(2)(B)(ii). In exchange, the United States agreed not to charge the defendant with various other offenses, supported by the factual basis, including Aggravated Identity Theft; to recommend the defendant receive a sentence within the advisory United States Sentencing Guidelines range as that range is determined by the Court on the date of sentencing; and to recommend certain special conditions of supervised release (or of probation should the Court impose a probationary sentence).

On April 10, 2017, the United States Probation Office issued a Presentence Investigation Report calculating the Adjusted Offense Level at 10, the Total Offense Level at 8 with acceptance, the Criminal History Category at I, and the advisory United States Sentencing Guidelines (USSG) range with acceptance at 0-6 months in Zone A. There are no objections to the Presentence Investigation Report. In accordance with the written Plea Agreement, the United States must recommend a sentence of no more than 6 months' incarceration. As explained below, the United States contends that a sentence of 6 months' incarceration is appropriate in light of the sentencing factors set forth in 18 U.S.C. § 3553(a).

ARGUMENT

The Court should incarcerate the defendant for six months. The United States anticipates that the defendant will advocate for a probationary sentence or home confinement. The Court is charged with imposing a sentence that is "sufficient, but not greater than necessary, to comply with the purposes" of sentencing set forth in

18 U.S.C. § 3553(a).[1] The requirement is "not merely that a sentencing court . . . be stingy enough to avoid [a sentence] that is too long, but also that it be generous enough to avoid one that is too short." *United States v. Irey*, 612 F.3d 1160, 1167 (11th Cir. 2010) (*en banc*). A sentence of six months' incarceration is appropriate in light of (1) the nature and circumstances of the offense; (2) the need for the sentence to reflect the seriousness of the offense, specifically the harm to the victims, promote respect for the law, and provide just punishment for the offense; (3) the need to deter future criminal conduct, by the defendant and others who are like minded; (4) the USSG and the kinds of sentences available; (5) and the need to avoid unwarranted sentencing disparities.

A. The Nature and Circumstances of the Offense

The recommended sentence of six months' incarceration appropriately reflects the nature and circumstances of the offense, specifically (1) the complex and repeated nature of the defendant's unauthorized access; (2) the number of, and

[1] Section 3553(a) requires the Court to consider the following factors in determining the appropriate sentence: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed (A) to reflect the seriousness of the offense, the promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; (3) the kinds of sentences available; (4) the kinds of sentence and sentencing range established by the Sentencing Guidelines; (5) any pertinent Guidelines policy statement; (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and (7) the need to provide restitution to any victims of the offense.

characteristics of, the victims affected; (3) the personal and intimate nature of the information accessed; and (4) the disturbing nature of the defendant's apparent motivations.

The defendant repeatedly and indiscriminately gained access to multiple women's computers for a period of at least two years using a number of methods in essence to stalk them. The defendant's primary tool to gain access to victim computers was phishing for victims' email account logins and passwords. In order to phish victims for email account information, the defendant spent countless hours creating numerous fictitious email accounts impersonating email administrators from multiple email providers; sending numerous emails from these accounts demanding login and password information; and then frequently checking the fictitious email accounts for response emails from victims. The defendant accessed and used his fictitious administrator email accounts at home and while traveling for work. But the defendant was not satisfied with the information he could obtain from phishing alone. The defendant also spent untold hours trolling the accounts he accessed via phishing for additional password information and conducting extensive open source research, for example on websites such as spokeo.com, on potential victims and making note of information about them including birthdates, places of employment, collegiate affiliations, etc. He then used this information to try and guess victims' passwords, or answer the security questions necessary to re-set them.

In some instances the defendant would re-set passwords multiple times in order to continue to access accounts after the victim had reset her password. The defendant accessed victim information across multiple platforms in this way including web based email, iCloud, and dropbox.

In all, based on the files on the defendant's hard drive and a sample of his phishing activity obtained by Google, the defendant victimized at least fifty women. He captured a few files from some victims and thousands from others. Because the defendant was not successful in accessing each account he attempted to access and because the defendant did not necessarily download and save data from each account he accessed and reviewed on his hard drive, it is impossible to truly know the number of victims or the amount of personal data involved.

The defendant was indiscriminate. He targeted women he knew and women he did not; women he had been romantically involved with and women he merely interacted with briefly; women with whom he had a connection, like a shared military history or high school and women who he found on the internet; and women who lived or worked near him in Shelby County, Alabama, and others who lived across the country and he was unlikely to ever see. The only thing that the defendant's victims had in common was the defendant's desire to delve into the details of their lives for his own pleasure.

Once the defendant was inside a victim's account, the defendant's primary motivation was to find photos of the victim nude or engaged in sexual activity, photos the victim had clearly intended for only a select other person or persons to see. But the defendant did not stop there. He downloaded other more wholesome images that allowed him to peek inside his victims' lives--images of children, pets, family parties, and nights on the town. He also turned his victims in to his accomplices, capturing their contacts to gain information about additional victims and trolling through their personal data and the intimate details of their electronic life to gain additional information that would allow him to access their other accounts. Finally, the defendant saved much of what he accessed to his hard drive to view again later, catalogued by victim or group for easier access.

The defendant's activity was not a whim or a single poor decision brought on by revenge or jealousy. This is not an instance where a spurned boyfriend successfully guesses his ex-girlfriend's email password and threatens to expose personal information. The defendant's actions were complex and pre-meditated and involved victims he did not know and had no reason to target. Although the defendant targeted many physically attractive women, it appears unlikely that the defendant was solely motivated by a desire to see pornographic images. The defendant could have obtained such images, and better images, far more easily with a basic internet search. The defendant's actions, instead appear to be based on an

intentional need to violate others privacy – as many others as he could. The defendant had no shame, going so far as to impersonate a victim in email and solicit obscene images from one of her contacts who had done nothing more than send her an old photo of the two on a boat trip. In light of the above nature and circumstances, a sentence of six months' incarceration is reasonable.

B. The Seriousness of the Offense, Respect for the Law, Just Punishment, and Deterrence

The recommended sentence of six months' incarceration also appropriately reflects the seriousness of the offense, provides respect for the law, provides just punishment and will adequately deter the defendant and others. These considerations reflect "the 'just deserts' concept, which carries the need for retribution, the need to make the punishment fit the crime, and the need not just to punish but to punish justly." *Irey*, 612 F.3d at 1206. The Eleventh Circuit has explained that "[b]ecause the punishment should fit the crime, the more serious the criminal conduct is the greater the need for retribution and the longer the sentence should be. The seriousness of the crime varies directly with the harm it causes or threatens. It follows that the greater the harm the more serious the crime, and the longer the sentence should be." *Id*.

The defendant's crime is serious, threatens harm, and must be deterred because of the current importance and prevalence of electronic data. Today, people live much of their lives electronically. Much of their personal communication and

their business, financial, educational, and healthcare correspondence is electronic, either via email, text messaging application, or social media platform messaging. People now take and store all their photographs and home videos digitally. As such people's email and online storage accounts now contain as much, if not more, intimate personal information about them as their homes do. In this age of digital living, passwords and security questions serve the same function as the lock on the front door once did. Computer intrusions are the new "break ins" and must be punished as such. Actions like the defendant's compromise email systems, decrease trust in technology, increase the security burdens imposed on everyone, and make it more difficult for people to access their accounts and their information, and quite simply live their lives. The Court must send the message to the defendant and others that these kinds of intrusions are serious and are not acceptable. This message is even more important in light of the fact that the desire to access improperly access digital information is outpacing society's technological ability to functionally password protect and encrypt it.

The defendant's crime is also serious because of the harm it caused to the specific victims in this case. If each of the defendant's intrusions was the equivalent of a "break in," the defendant's repeated intrusions across multiple platforms and his cataloging of the victim's information for his own later use and pleasure was the equivalent of a stalking. When the victims in this case learned of the defendant's

activity they told law enforcement they felt violated, embarrassed about the things the defendant had seen, and scared for themselves and their children. They felt unsafe using their computers or other technological platforms. Like victims of other intimate act crimes, they did not want to publicly talk about the offense or write to the court; they simply wanted to forget that it ever happened. Such a crime must be labeled as serious and punished as such, or it will continue to occur.

C. The Sentencing Guidelines and Kinds of Sentences Available

The recommended sentence of six months' incarceration, at the top of the Guidelines range, is appropriate in light of the Sentencing Guidelines and the kinds of sentences available. The Guidelines allow for a sentence of six months' incarceration but allow for a probationary sentence or a sentence of home confinement as well. Such sentences would not be appropriate considering the Guidelines failure to fully capture the non-financial harm caused in this case.

Violations of 18 U.S.C. § 1030 are largely sentenced under U.S.S.G. 2B1.1. This Guideline is directed primarily at fraud and theft offenses, and the advisory Guideline ranges generated by this Guideline are heavily influenced by the financial loss amount. The zero to six-month advisory Guideline range in the instant case is driven largely by the lack of loss – or the lack of a financial component to the case. The defendant's intrusion did not cause extensive reported damage to the victims' hardware or software that cost money to repair; the defendant did not engage in his

offense for financial gain; and the information the defendant took did not have financial value, as it might have had, for example, if the defendant had downloaded trade secrets, or even nude images of celebrities. As a result, the defendant received no additional points in the Guidelines under 2B1.1(b)(1).

The Eleventh Circuit has recognized that USSG 2B1.1 does not always adequately account for non-financial harms, including invasion of privacy, in computer intrusion cases. *United States v. Feigin*, 365 Fed. Appx. 180 (11th Cir. 2010). In *United States v. Feigin* the defendant pled guilty to one count of violating 18 U.S.C. § 1030(a)(2) and (c)(2)(B)(ii) and admitted to (1) installing webcam spy software on the computer of a female victim; (2) using the software to control the web camera on the victim's computer and automatically view, record and photograph her activities without her knowledge or consent, including recording her and others in various stages of undress; and (3) hosting over 10,000 images of the victim on a foreign server and using them to advertise the webcam spy software to others. 365 Fed. Appx. at 181. The victim testified at sentencing that she knew Feigin and had given him access to her computer to assist her with it; she received distasteful comments from individuals viewing the website; and she suffered emotional and psychological harm. *Id.* at 182. The probation officer calculated Feigin's total offense level as twelve based on two point enhancements for use of a special skill (computer skills) and relocation of the offense to another jurisdiction to

avoid detection (use of the foreign server). *Id.* at 181-82. Feigin had a criminal history category of one, so his Guidelines range was ten to sixteen months. *Id.* at 182. Feigin argued for time served of three weeks and supervised release. *Id.* Pursuant to the plea agreement, the United States did not advocate for a specific sentence but pointed out to the court how the Guidelines are designed to address financial harm rather than invasion of privacy. *Id.* The court varied upward and sentenced Feigin to thirty months on the basis that the Guidelines did not adequately account for the harm to the victim. *Id.* at 183. The Eleventh Circuit affirmed the sentence as substantively reasonable in light of the seriousness of the offense, as illustrated by the harm to the victim, and the need to insure adequate deterrence for others who might contemplate similar conduct. *Id.* at 188.

The instant case presents less of a privacy concern than *Feigin* because it does not involve distribution of victim images or direct contact with the victim; however, it presents greater concerns than *Feigin* in the sense that it involves over fifty victims, rather than one, involves repeated and varied computer intrusions rather than one computer intrusion, and involves data in addition to photographs. The United States is not asking the Court to vary upward as it did in *Feigin*, it is simply asking the Court to impose the maximum Guidelines sentence to account for the privacy concerns that are not fully addressed in the Guidelines.

D. The Need to Avoid Unwarranted Sentencing Disparities

The requested sentenced of six months' incarceration is reasonable in light of the sentences imposed in factually similar cases and the need to avoid unwarranted sentencing disparities. The undersigned is aware of two similar cases.

In *United States v. Hunter Moore*, 2:13-cr-00917 (C.D. Cal.), the defendant was charged with aggravated identity theft in violation of 18 U.S.C. § 1029(a), conspiracy in violation of 18 U.S.C. § 371, and unauthorized computer access in violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i) (Indictment, Docket Entry 1). He encouraged a co-conspirator to "hack" in to victims' Google email accounts using their usernames and passwords and obtain nude images; paid the co-conspirator for the images he obtained; and posted them on a website Moore operated and maintained (*Id.*). Moore pled guilty and was sentenced to 30 months' incarceration – six months as to the intrusion count and the mandatory 24 months as to the aggravated identity count (Plea, Docket Entry 47; Judgement and Commitment, Docket Entry 110).

In *United States v. Ryan Collins*, 2:16-cr-00157 (C.D. Cal), 1:16-cr-00121 (M.D. Pa.), the defendant agreed to plead guilty to a one-count Information charging unauthorized computer intrusion in violation of 18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(ii) and (iii) (Plea, Docket Entry 5). He admitted to accessing the Apple iCloud and Gmail accounts of over 100 victims, including many female celebrities,

without their authorization, and obtaining photographs and other private information valued over $5000. (*Id.*). The parties agreed that two-point enhancements for ten or more victims, sophisticated means, and seeking personal information would apply. (*Id.* ¶ 11.) With these enhancements, the Guidelines range was 10-16 months without acceptance and 6-12 months with acceptance, however, the parties agreed to a sentence of 18 months' incarceration based in large part on the Government's agreement not to charge the defendant with aggravated identity theft for the use of the victim's login information. (*Id.* ¶ 12.) At sentencing the parties provided additional information about the crime, including that (1) the defendant had been involved in a phishing scheme; (2) the defendant had been involved in a scheme to convince non-celebrity victims to send him nude photographs by pretending to offer modeling opportunities; (3) the defendant did not post or forward the photos he obtained; (4) the defendant did not attempt to benefit financially from any photographs in his possession; (5) the United States identified over 600 victims, many celebrities, 50-100 of which had at least one nude photograph stolen. (Sentencing Memorandums, Docket Entries 22 and 24.) The court agreed with the parties and imposed a sentence of 18 months' incarceration and two years of supervised release, which included computer monitoring and a mental health assessment. (Judgement and Conviction, Docket Entry 27).

Unlike the instant case, *Moore* involved the ultimate sharing of the victims' images, otherwise the cases are factually similar. The factual basis in *Collins* is remarkable similar to the instant case. Like the defendant, both Moore and Collins were a criminal history category I. To avoid creating an unwarranted sentencing disparity the Court should impose a sentence of incarceration. A sentence of six months' incarceration is reasonable in light of the facts of these other matters.

E. The Need for the Government's Special Conditions

The special conditions requested by the United States should be imposed as part of any period of probation or supervised release. Special conditions of supervised release or probation should be reasonably related to the factors in 18 U.S.C. § 3553(a), involve no greater deprivation of liberty than is reasonably necessary, and be consistent with the policy statements of the Sentencing Commission. 18 U.S.C. § 3583(d). The United States recommends the following special conditions apply to any period of supervised release or probation imposed by the Court: (1) the defendant participate in regular mental health treatment; (2) the defendant complete 250 hours of community service; (3) the defendant consent to random technology monitoring by probation; and (4) within ninety (90) days of sentencing, the defendant prepare an apology letter to the victims to be provided to the United States' Attorney's Office for distribution.

Mental health treatment for the defendant is consistent with section 3553(a) and the Guidelines and is reasonably related to the offense in light of the nature and circumstances of the offense and the defendant's seemingly disturbing motivation for committing it. Community service is reasonably related to the need to adequately punish the offense and provide deterrence. Should the defendant receive the probationary sentence requested by the defense or the brief sentence of incarceration requested by the United States, community service is necessary ensure the defendant feels the consequences of his actions in a tangible way. Technology monitoring is necessary in light of the nature and circumstances of the offense in order to protect the public from future crimes. As noted above the harm caused in this case is largely emotional and psychological and cannot be remedied with traditional monetary restitution. The apology letter is one mechanism to ensure that the victims are appropriately compensated for their harm.

CONCLUSION

For the reasons stated above, the United States recommends a sentence of six months' incarceration at the high end of the advisory sentencing Guidelines range; restitution as appropriate; and a period of supervised release with special conditions. This sentence is consistent with the purposes of sentencing in section 3553(a) and is sufficient but no greater than necessary.

Respectfully submitted this the 12th day of May, 2017,

/s/ Electronic Signature
ROBERT O. POSEY
Acting United States Attorney

ERICA WILLIAMSON BARNES
Assistant United States Attorney

CERTIFICATE OF SERVICE

I certify that on this the 12th day of May, 2017, I filed a copy of the above pleading electronically using CM/ECF which will send notice to all counsel of record.

/s/ Electronic Signature
ERICA WILLIAMSON BARNES
Assistant United States Attorney